

JUN 14 2019

(USAO GAN 6/10) Search Warrant

JAMES N. HATTEN, Clerk

By: *Kari Bull*

United States District Court

NORTHERN DISTRICT OF GEORGIA

In the Matter of the Search of

Information associated with cellular phone number 770-549-6127 that is stored at premises owned, maintained, controlled, or operated by Sprint Corporation, a company with an office at 6480 Sprint Parkway, Overland Park, KS

APPLICATION AND
AFFIDAVIT FOR
SEARCH WARRANT
Case number: 4:19-mc-34-WEJ

I, Russell Dellinger, being duly sworn depose and say:

I am a Special Agent of the Federal Bureau of Investigation and have reason to believe that on the property described as:

Information associated with cellular phone number 770-549-6127 that is stored at premises owned, maintained, controlled, or operated by Sprint Corporation, a company with an office at 6480 Sprint Parkway, Overland Park, KS

There is now concealed certain property, certain information, and certain data, namely,

SEE ATTACHMENT A

which constitutes evidence of a crime, concerning violations of Title 18, United States Code, Sections 1343 and 1349, over which the United States District Court for the Northern District of Georgia has jurisdiction. The facts to support a finding of Probable Cause are as follows:

SEE ATTACHED AFFIDAVIT

Continued on attached sheet made a part hereof.

Sworn to before me, and subscribed in my presence

June 14, 2019

Date

WALTER E. JOHNSON
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer

AUSA Samir Kaushal

R. M. Dellinger
Signature of Affiant

Russell Dellinger

Rome, Georgia

City and States

Walter E. Johnson
Signature of Judicial Officer

Attachment A
Information to be Disclosed by the Provider

For the account identified as and/or associated with: **Sprint Corporation cellular telephone assigned phone number 770-549-6127**, Sprint is required to disclose the following information to the government:

- a. All business records and subscriber information, in any form kept, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;
- b. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number);
- c. All transactional information of all activity, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from October 1, 2018, until present;
- d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message October 1, 2018, until present;
- e. Detailed billing records, showing all billable calls including outgoing digits, from October 1, 2018, until present;

- f. All records of internet activity, including session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, from October 1, 2018, until present;
- g. Historical cell site/ sector data, including: (i) the cell sites to which the Subject Telephone sent its signal when a call, text message, or data transmission was made, placed, or received; (ii) the cell sites through which the call or data transmission were routed when the call or data transmission ended; and (iii) the cell sites during a call or data transmission, if available, from October 1, 2018, until present; and
- h. Per-call measurement data (also known as "PCMD") from October 1, 2018, until present.

Sprint is hereby ordered to provide an engineering map showing cell-site tower locations, sectors, and orientations. All records described above shall be provided in an electronic format within 14 days of the date of this warrant and shall be accompanied by a Business Records Certification.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, Russell Dellinger, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of applications for search warrants under Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. § 2703(c)(1)(A) to require Verizon Wireless and Sprint Corporation to disclose to the government records and information pertaining to the following accounts, together referred to as the Subject Telephones, stored at premises owned, maintained, controlled, or operated by the providers:

- a) Subject Telephone 1: Verizon Wireless telephone 404-998-7197, believed to be used by **Gerald McCarty**.
- b) Subject Telephone 2: Sprint telephone 770-549-6127, believed to be used by **Tiffany McNamara**.

This warrant does not seek disclosure of contents of communications.

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the users of the Subject Telephones, **McCarty** and **McNamara**, committed multiple wire frauds in the Northern District of Georgia, in violation of 18 U.S.C. §§ 1343 (wire fraud) and 1349 (wire fraud conspiracy), and that the requested records, described more particularly in Attachment A, contain evidence of such violations.

3. This Court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction,” as defined in 18 U.S.C. § 2711(3). *See* 18 U.S.C. § 2703(d). Specifically, the Court has jurisdiction over the offenses being investigated. *See* 18 U.S.C. § 2711(3)(A)(i). Verizon Wireless and Sprint are each providers of electronic communications services, as defined in 18 U.S.C. § 2510(15). Verizon

Wireless maintains an office in Bedminster, New Jersey, and Sprint maintains an office in Overland Park, Kansas.

4. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since January 2018. I am currently assigned to the FBI Atlanta Field Office, Rome Resident Agency, responsible for investigating all criminal and civil violations of the laws of the United States, including wire fraud. I have experience reviewing telephone call detail records, including records related to historical cell site information, Global Position System (GPS), Enhanced 911, specific latitude and longitude, and other precise location information for cellular telephones.

Probable Cause

5. The FBI is investigating a wire fraud scheme that was executed in Hiram, Georgia, between October 19 and 30, 2018. According to the investigation to date, the victim, Jason Brackeen, was duped into paying \$80,000 to **McCarty** for a generator that was never delivered. The information contained in this probable cause statement was provided by Brackeen.

6. On 10/19/2018:

- a) Brackeen received an email from a business associate, John Larson, about **Gerald McCarty** offering a Cummins KTA50-G9 Diesel Generator for sale;
- b) Brackeen contacted **McCarty** telephonically and via text message, referencing his interest in the generator. All telephonic and text message contact Brackeen had with **McCarty** from the beginning of the communications (10/19/2018), through the present, were and continue to be via Subject Telephone 1;

- c) Brackeen and **McCarty** spoke telephonically about the generator and verbally agreed to a sale price of \$137,500, subject to inspection by Brackeen; and
- d) Brackeen emailed to **McCarty** confirmation of the agreed sale amount and requested an invoice from **McCarty**.

7. On 10/21/2018:

- a) Brackeen booked a flight from Dallas, TX, to Charlotte, NC, and rental car for travel to the generator inspection location in McLeansville, NC.
- b) **McCarty** sent an email stating he would have the invoice later that day and his secretary, **McNamara**, would send the invoice.
- c) Brackeen requested an IRS Form W9 for **McCarty's** company, Coast to Coast LLC, and the trailer VIN from **McCarty**. **McCarty** agreed, and stated he expected a wire transfer for payment.

8. On 10/22/2018, Brackeen received an invoice and IRS Form W9 from **McNamara** via email. **McNamara** called Brackeen from Subject Telephone 2 to confirm that they were received. That same day, Brackeen flew from Dallas, TX, to Charlotte, NC.

9. On 10/23/2018, Brackeen inspected the generator in North Carolina. Brackeen took pictures of the generator, confirmed serial numbers, and performed a complete inspection. During the inspection, Brackeen identified multiple issues with the generator and stated that he would not be able to pay the agreed upon price due to its condition. Brackeen left with no intention of purchasing the generator set, but did request a video once **McCarty** was able to get the generator started.

10. On 10/26/2018, **McCarty**, via telephone, told Brackeen that he had gotten the generator running and that it ran good. **McCarty** sent a video of the generator running to Brackeen. **McCarty** also told Brackeen that he would take \$80,000 for the generator. Brackeen agreed to the price and sent a revised invoice to **McCarty** and **McNamara**.

Brackeen wired \$10,000 to **McCarty** at Regions Bank in Hiram, GA, as instructed on the original invoice. **McCarty** confirmed receipt of the funds with Brackeen via text message.

11. On 10/28/2018, Brackeen and **McCarty** agreed that **McCarty** would transport the generator from North Carolina to Texas for an additional \$3,000. Brackeen received an invoice for \$3,000 from **McNamara**.

12. On 10/30/2018, Brackeen wired the balance of the price of the generator, \$70,000, to **McCarty**. **McCarty** confirmed receipt of the funds via text message.

13. Between 10/30/2018 and 11/5/2018, **McCarty** provided multiple delivery dates to Brackeen over the phone but no delivery was completed.

14. On 11/5/2018, **McCarty** told Brackeen it would be 11/7/2018 before the generator would be delivered because **McCarty** had a death in his immediate family.

15. On 11/12/2018, **McCarty** informed Brackeen that he was having issues with the truck and that Brackeen will not owe the \$3,000 for delivery.

16. On 11/27/2018, Brackeen sent **McCarty** an email with his bank wiring instructions and requested that **McCarty** return the \$80,000. **McCarty** replied to the email confirming receipt of the wiring instructions.

17. On 12/11/2018, Brackeen sent a demand letter to **McCarty** with return receipt requested.

18. On 2/1/2019, Brackeen confirmed with the management of business where the generator was inspected that the generator was in the same location as during the inspection and had not been moved.

19. As of 5/22/2019, Brackeen has maintained communication with **McCarty** and requested that the \$80,000 be returned. **McCarty** has promised to repay the money multiple times, always stating that he needs more time.

20. Based on the foregoing, there is probable cause to believe the requested records, described with particularity in Attachment A, will yield evidence of fraud

committed by the users of the Subject Telephones, in violation of 18 U.S.C. §§ 1343 and 1349.

Cellular Phones & Cell Site Data

21. Cellular service providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

22. Cellular service providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Station Equipment Identity (“IMEI”). When a cellular device connects to a cellular antenna or tower, it reveals its

embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

23. Sprint and Verizon Wireless retain information about the location from which a particular communication was transmitted or received. This information can include data about which “cell towers” (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question. Based on my training and experience, I know that Sprint and Verizon Wireless also can collect per-call measurement data (“PCMD”) which estimates the approximate distance of the cellular device from a cellular tower based upon the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

24. Cellular service providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers’ full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers’ Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, cellular service providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

25. Information stored at the cellular service provider, including that described above, may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such “timeline” information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site and PCMD location information).

Conclusion

26. Based on the foregoing, I request that the Court issue the proposed search warrants under 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41. I further request that the Court direct Verizon Wireless and Sprint to disclose to the FBI any information described in Attachment A that is within its possession, custody, or control. Because the warrants will be served on Sprint and Verizon Wireless, who will then compile the requested records at a time convenient to them, reasonable cause exists to

permit the execution of the requested warrants at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of the warrants.